Рис. 1. Принципиальная схема дубликатора

Исходя из полученных данных можно сделать однозначный вывод о возможности и целесообразности создания аппаратного дубликатора на основе программируемого микроконтроллера с заявленным функционалом для небольших негосударственных экспертных учреждений. Считаем необходимым дальнейшее исследование данного вопроса и разработка прототипа дубликатора.

Список литературы

1. Федеральный закон от 31.05.2001 № 73-ФЗ (ред. от 08.03.2015) «О государственной судебно-экспертной деятельности в Российской Федерации».

2. *Menz M.*, *Bress S.* The Fallacy of Software Write Protection in Computer Forensics // MyKey Technology Inc. URL: http://mykeytech.com/softwarewriteblocking2-4.pdf (дата обращения: 15.11.2017).

3. *Прокопенко С.* Проблемы копирования данных с накопителей с дефектными секторами при производстве компьютерно-технических экспертиз // Лаборатория компьютерной криминалистики ЕПОС. URL: http://www.epos.ua/cp/pf/publications/data/upimages/imaging-bad-sectors-computer-forensics_prokopenko.pdf (дата обращения: 15.11.2017).

УДК 004.056

В. Ю. Кобяков, А. С. Лучинин, О. Н. Бузмакова
Научный руководитель: канд. тех. наук, доцент А. С. Лучинин
Уральский федеральный университет, Екатеринбург

ИССЛЕДОВАНИЕ ИНФОРМАТИВНОСТИ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ, СОЗДАВАЕМОГО СКАНЕРОМ ШТРИХ-КОДОВ

Аннотация. В статье рассмотрена возможность корреляционной оценки информативности побочного электромагнитного излучения на примере сканера штрих-кодов. Полученные практические результаты доказывают обоснованность и целесообразность предложенного метода.

Ключевые слова: ПЭМИ; электромагнитное излучение; техническая защита информации.

Современный уровень развития радиоэлектронной аппаратуры специального назначения позволяет принимать, фильтровать и обрабатывать сигналы даже при отрицательном отношении сигнал/шум [1]. Принимая во внимание данное обстоятельство и возможные перспективные разработки аппаратуры перехвата, в методических пособиях по проведению специальных исследований задается очень жесткий критерий по уровням побочных электромагнитных излучений. И вполне обоснованно имеется ряд публикаций, в которых описываются успешные опыты по радиоперехвату. Знаменитый Вим ван Эйк еще в далеком 1985 году наглядно продемонстрировал возможность перехвата информации с ЭЛТ-мониторов [2]. Маркус Кун в 2004 году осуществил перехват изображения с ЖК-монитора [3], а в 2008 году группа швейцарских исследователей продемонстрировала перехват информации с клавиатуры [4] с наглядным роликом в YouTube [5]. Вопросом побочного электромагнитного излучения занимались многие ученые, и эта проблема актуальна в настоящее время.

Коммерческие организации в целях сокращения расходов часто не руководствуются требованиями государственных, национальных и иных стандартов по электромагнитной совместимости при проектировании радиоэлектронных устройств. Результатом данного подхода может являться невозможность эксплуатации данных устройств в целях оборонных ведомств, а также при обработке информации, защищаемой государством [6].

Например, для внедрения сканера штрих-кодов в технологические процессы предприятия и использования в выделенном помещении необходимо соблюдение требований ФСТЭК и ФСБ по побочным электромагнитным излучениям. Требуемая зона R2 должна составлять менее 10 метров. Расчет должен проводиться по закрытой методике, но из-за отсутствия доступа к выше указанной литературе было сказано, что действующая зона радиоизлучения составляет 150 метров.

Для определения требуемого уровня подавления примем модель распространения радиоволн в дальней зоне, где уровень электрической составляющей излучения обратно пропорционально расстоянию $P \sim 1/S$.

Зная зависимость затухания сигнала от расстояния и радиусы действующей и требуемой зон R2, уровень подавления можно вычислить по формуле:

$$Q = 20 \cdot \log_{10}\left(\frac{R2_{\text{наст}}}{R2_{\text{треб}}}\right) \qquad (1)$$

$$Q = 20 \cdot \log_{10}\left(\frac{150}{10}\right) \approx 24 \text{ Дб}.$$

24 дБ по напряженности электрического поля — огромное значение, добиться которого минимальными техническими доработками практически невозможно. Необходимо создать новое устройство, отвечающее требованиям по ПЭМИ или доказать отсутствие информативной составляющей в излучаемом сигнале. Перед нами была поставлена задача изучения побочного электромагнитного излучения от сканера штрих-кодов.

Была выдвинута гипотеза, что источником излучения дискретных гармоник в широком диапазоне частот является тактовый генератор, который модулирует низкочастотные сигналы строчной развертки (20 кГц) и DC/DC-преобразователя (900 кГц). Генератор строчной развертки излучает постоянно при считывании видеокамерой изображения и не несет в себе никакой информации о нем. DC/DC-преобразователь начинает работать при подаче питания на прибор и не связан с обрабатываемой информацией. Если около несущей гармоники не будет обнаружено никаких других низкочастотных составляющих, кроме описанных выше, и характер гармоник не будет динамически изменяться от обрабатываемой информации, то достоверно будет доказано отсутствие информативности ПЭМИ.

Исследуемый сканер штрих-кодов состоит из видеокамеры, вычислительного процессора и интерфейса вывода на компьютер. Камера фотографирует картинку с штрих-кодом, передает его процессору, который по изображению вычисляет код и передает его по интерфейсу RS232 или USB на компьютер. Из-за особенности технической реализации устройства его необходимо тестировать как видеосистему.

Для проверки выдвинутой гипотезы был проведен эксперимент, целью которого было доказательство наличие корреляционной составляющей между излучаемым сигналом ПЭМИ и обрабатываемым изображением. Обнаружив наиболее мощный сигнал, излучаемый устройством, были проанализированы его боковые составляющие на наличие различий в зависимости от подаваемого на камеру изображения.

Измерения проводились в безэховой камере Института радиоэлектроники и информационных технологий УрФУ, которая имеет уровень подавления внешних радиоизлучений 100 дБ, что позволяет гарантировано исключить посторонние сигналы. Прибор был подключен к ноутбуку, и для исключения ПЭМИ от него была предложена следующая хитрость:

1) настраивался сканер и ноутбук на передачу видео;

2) ноутбук разряжался и уходил в режим гибернации, сканер при этом продолжал работать и в холостую передавать изображение;

3) проводились измерения;

4) запускался ноутбук, и «просыпалась» программа на получение изображения.

Измерения проводились в безэховой камере на расстоянии трех метров анализатором спектра реального времени, который параллельно сканирует полосу обзора. Для эксперимента использовалось четыре типа изображений:

1) камера заклеена, абсолютная темнота. Изображение на мониторе компьютера — серый шумообразный фон. Спектр *а*;

2) камера направленна на белый лист бумаги. Изображение на мониторе — серая картинка. Спектр *б*;

3) 7 вертикальных полосок. Картинка начинается с черной полосы, заканчивается белой. Спектр *в*;.

4) 2 черных полоски. Начинается с белой полосы, заканчивается тоже белой. Спектр *г*.

Наиболее сложно различить друг от друга спектры с черным фоном и семью черно-белыми полосами (рис. 1). Остальные формы спектра отчетливо можно отличить друг от друга. Все боковые составляющие кратны 20 кГц, имеется небольшое число дискретных гармоник с частотой 10 кГц. Множество кратных гармоник объясняется импульсной формой несущего сигнала.

Полученные спектры не позволяют достоверно определить характер изображения, потому что при семи вертикальных полосах при частоте строчной развертки 20 кГц должна наблюдаться частота, в семь раз превышающая строчную развертку, то есть около 140 кГц.

Принципиально новых гармонических составляющих не было обнаружено, все гармоники связаны с частотой строчной развертки. Изменение энергетических и частотных характеристик низкочастотного сигнала при различных

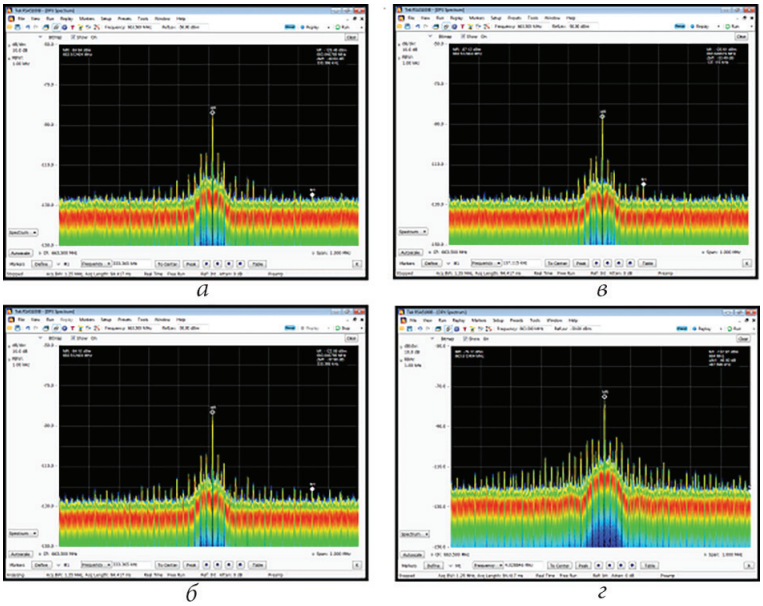

Рис. 1. Спектр ПЭМИ при различных изображениях

изображениях, подаваемых на видеокамеру, свидетельствует о наличии взаимосвязи между обрабатываемой информацией и ПЭМИ. Следовательно, побочное электромагнитное излучение от сканера штрих-кодов является информативным и теоретически из него можно извлечь информативную составляющую.

Поставленная перед нами задача решена, но необходимы дальнейшие исследования для выделения информативного сигнала и практического подтверждения теоретических результатов.

Список литературы

1. *Сребнев В. И.* Поисковый радиомониторинг: проблемы, методики, аппаратура // Системы безопасности. 1999. 24. Январь-февраль. С. 58–63.

2. *Van Eck W*. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? // Computers & Security : journal. Elsevier Advanced Technology Publications, 1985. Vol. 4, Is. 4. P. 269–286. ISSN01674048. DOI: 10.1016/0167–4048(85)90046-X.

3. *Markus G*. Kuhn Security Limits for Compromising Emanations // Cryptographic Hardware and Embedded Systems. 2005. Vol. 3659. P. 265–279. DOI: 10.1007/11545262_20.

4. *Vuagnoux M*., *Pasini S.* Compromising electromagnetic emanations of wired and wireless keyboards // Proceeding SSYM'09 Proceedings of the 18th conference on USENIX security symposium. 2009. P. 1–16

5. juhztfzujb. Compromising electromagnetic emanations of wired keyboards 2 [Любительское видео] // YouTube. 23 октября 2008. https://youtu.be/d926EztWimM (дата обращения: 15.09.2017).

6. ФЗ № 162-ФЗ «О стандартизации в Российской Федерации» (с изменениями и дополнениями) от 29 июня 2015 г. [Электронный ресурс]. 2015. Режим доступа: http://www.gost.ru/wps/wcm/connect/43debd0048f477a5a38dfb-56779c92ad/FZ_29.06.2015_162.pdf? MOD=AJPERES

УДК 004

М. Н. Вольхина, К. Л. Стойчин
Научный руководитель: д-р тех. наук, проф. С. В. Поршнев
Уральский федеральный университет, Екатеринбург

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСУ ТП

Аннотация. В настоящее время автоматизированные системы управления технологическими процессами (далее — АСУ ТП) имеют широкое распространение в промышленной и производственной сфере. Применение АСУ ТП охваты-